

PCT/JP 2004/016708

日 本 国 特 許 庁
JAPAN PATENT OFFICE

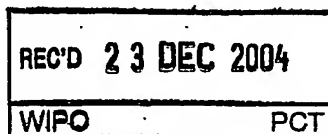
04.11.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 4 年 2 月 1 3 日
Date of Application:

出 願 番 号 特 願 2 0 0 4 - 0 3 7 3 1 4
Application Number:
[ST. 10/C] : [J P 2 0 0 4 - 0 3 7 3 1 4]



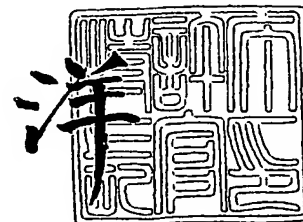
出 願 人 エヌ・ティ・ティ・コミュニケーションズ株式会社
Applicant(s):

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2 0 0 4 年 1 2 月 1 3 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



BEST AVAILABLE COPY

出証番号 出証特 2 0 0 4 - 3 1 1 3 6 6 1

【書類名】 特許願
【整理番号】 GLN00462
【提出日】 平成16年 2月13日
【あて先】 特許庁長官 今井 康夫 殿
【国際特許分類】 G06F 17/00
H04L 12/22

【発明者】
【住所又は居所】 東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミ
ユニケーションズ株式会社内
【氏名】 齊藤 充

【発明者】
【住所又は居所】 東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミ
ユニケーションズ株式会社内
【氏名】 山崎 俊之

【発明者】
【住所又は居所】 東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミ
ユニケーションズ株式会社内
【氏名】 宮川 晋

【発明者】
【住所又は居所】 東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミ
ユニケーションズ株式会社内
【氏名】 江頭 孝

【発明者】
【住所又は居所】 東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミ
ユニケーションズ株式会社内
【氏名】 鈴木 俊明

【発明者】
【住所又は居所】 東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミ
ユニケーションズ株式会社内
【氏名】 内山 貴充

【特許出願人】
【識別番号】 399035766
【氏名又は名称】 エヌ・ティ・ティ・コミュニケーションズ株式会社

【代理人】
【識別番号】 100070150
【弁理士】
【氏名又は名称】 伊東 忠彦

【手数料の表示】
【予納台帳番号】 002989
【納付金額】 21,000円

【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1

【書類名】 特許請求の範囲**【請求項 1】**

第 1 の装置及び第 2 の装置とネットワークを介して接続する手段を備えたセッション管理装置であって、

第 1 の装置との間で相互認証を行い、セッション管理装置と第 1 の装置との間で第 1 の暗号化通信チャネルを確立し、第 1 の装置の名前と第 1 の暗号化通信チャネルの識別情報とを対応付けて保持する手段と、

セッション管理装置と第 2 の装置との間で相互認証に基づく第 2 の暗号化通信チャネルを確立する手段と、

第 1 の装置から、第 1 の装置の名前を含むメッセージを、第 1 の暗号化通信チャネルを介して受信し、当該メッセージに含まれる第 1 の装置の名前と、第 1 の暗号化通信チャネルの識別情報と対応付けて保持されている第 1 の装置の名前とを比較することにより、メッセージに含まれる第 1 の装置の名前が正しいか否かを判定する手段と、

そのメッセージを第 2 の暗号化通信チャネルを介して第 2 の装置に送信する手段とを有することを特徴とするセッション管理装置。

【請求項 2】

前記メッセージに含まれる第 1 の装置の名前が正しくないと判定した場合に、エラーメッセージを第 1 の装置に送信する請求項 1 に記載のセッション管理装置。

【請求項 3】

第 1 の装置及び第 2 の装置とネットワークを介して接続する手段を備えたセッション管理装置であって、

第 1 の装置との間で相互認証を行い、セッション管理装置と第 1 の装置との間で第 1 の暗号化通信チャネルを確立する手段と、

セッション管理装置と第 2 の装置との間で相互認証に基づく第 2 の暗号化通信チャネルを確立する手段と、

第 1 の装置から、第 1 の装置とセッション管理装置間の経路の信頼性を示すヘッダを含むメッセージを、第 1 の暗号化通信チャネルを介して受信する手段と、

セッション管理装置と第 2 の装置との間の経路の信頼性を示すヘッダを前記メッセージに追加し、そのメッセージを第 2 の暗号化通信チャネルを介して第 2 の装置に送信する手段と

を有することを特徴とするセッション管理装置。

【請求項 4】

前記メッセージに含まれる前記経路の信頼性を示すヘッダは、当該ヘッダを付した装置のアドレスを含み、当該メッセージを受信すると、そのヘッダに含まれるアドレスと、当該メッセージを送信した送信元の装置のアドレスとを比較することにより、当該ヘッダの正当性を判定する請求項 3 に記載のセッション管理装置。

【請求項 5】

前記メッセージは SIP に基づくメッセージである請求項 1 ないし 4 のうちいずれか 1 項に記載のセッション管理装置。

【請求項 6】

ネットワークに接続された第 1 の装置、セッション管理装置、及び第 2 の装置の間でメッセージを転送する方法であって、

セッション管理装置と第 1 の装置との間で相互認証を行い、セッション管理装置と第 1 の装置との間で第 1 の暗号化通信チャネルを確立し、セッション管理装置が、第 1 の装置の名前と第 1 の暗号化通信チャネルの識別情報とを対応付けて保持するステップと、

セッション管理装置と第 2 の装置との間で相互認証に基づく第 2 の暗号化通信チャネルを確立するステップと、

第 1 の装置が、第 1 の装置の名前を含むメッセージを第 1 の暗号化通信チャネルを介してセッション管理装置に送信するステップと、

セッション管理装置が、前記メッセージに含まれる第 1 の装置の名前と、第 1 の暗号化

通信チャネルの識別情報と対応付けて保持されている第1の装置の名前とを比較することにより、前記メッセージに含まれる第1の装置の名前が正しいか否かを判定するステップと、

そのメッセージを第2の暗号化通信チャネルを介して第2の装置に送信するステップとを有することを特徴とする方法。

【請求項7】

セッション管理装置は、前記メッセージに含まれる第1の装置の名前が正しくないと判定した場合に、エラーメッセージを第1の装置に送信する請求項6に記載の方法。

【請求項8】

ネットワークに接続された第1の装置、セッション管理装置、及び第2の装置の間でメッセージを転送する方法であって、

セッション管理装置と第1の装置との間で相互認証を行い、セッション管理装置と第1の装置との間で第1の暗号化通信チャネルを確立するステップと、

セッション管理装置と第2の装置との間で相互認証に基づく第2の暗号化通信チャネルを確立するステップと、

第1の装置が、第1の装置とセッション管理装置間の経路の信頼性を示すヘッダを含むメッセージを、第1の暗号化通信チャネルを介してセッション管理装置に送信するステップと、

セッション管理装置が、セッション管理装置と第2の装置との間の経路の信頼性を示すヘッダを追加した前記メッセージを第2の暗号化通信チャネルを介して第2の装置に送信するステップと

を有することを特徴とする方法。

【請求項9】

第2の装置は、前記メッセージに付された経路の信頼性を示すヘッダを参照して、前記メッセージが信頼できるものであるか否かの判定を行う請求項8に記載の方法。

【請求項10】

第2の装置は、当該第2の装置が受信したメッセージに付された経路の信頼性を示す一連のヘッダと同じ一連のヘッダを含む応答メッセージを前記セッション管理装置に送信する請求項8又は9に記載の方法。

【請求項11】

前記メッセージに含まれる前記経路の信頼性を示すヘッダは、当該ヘッダを付する装置のアドレスを含み、当該メッセージを受信した装置は、そのヘッダに含まれるアドレスと、当該メッセージを送信した送信元の装置のアドレスとを比較することにより、当該ヘッダの正当性を判定する請求項8に記載の方法。

【請求項12】

前記メッセージはSIPに基づくメッセージである請求項6ないし11のうちいずれか1項に記載の方法。

【請求項13】

コンピュータを、ネットワークに接続された第1の装置と第2の装置との間でメッセージ送受信を行うセッション管理装置として機能させるプログラムであって、コンピュータを、

第1の装置との間で相互認証を行い、第1の装置との間で第1の暗号化通信チャネルを確立し、第1の装置の名前と第1の暗号化通信チャネルの識別情報とを対応付けて保持する手段、

第2の装置との間で相互認証に基づく第2の暗号化通信チャネルを確立する手段、

第1の装置から、第1の装置の名前を含むメッセージを、第1の暗号化通信チャネルを介して受信し、当該メッセージに含まれる第1の装置の名前と、第1の暗号化通信チャネルの識別情報と対応付けて保持されている第1の装置の名前とを比較することにより、メッセージに含まれる第1の装置の名前が正しいか否かを判定する手段、

そのメッセージを第2の暗号化通信チャネルを介して第2の装置に送信する手段

として機能させるプログラム。

【請求項 14】

コンピュータを、ネットワークに接続された第 1 の装置と第 2 の装置との間でメッセージ送受信を行うセッション管理装置として機能させるプログラムであって、コンピュータを、

第 1 の装置との間で相互認証を行い、第 1 の装置との間で第 1 の暗号化通信チャネルを確立する手段、

第 2 の装置との間で相互認証に基づく第 2 の暗号化通信チャネルを確立する手段、

第 1 の装置から、第 1 の装置とセッション管理装置間の経路の信頼性を示すヘッダを含むメッセージを、第 1 の暗号化通信チャネルを介して受信する手段、

第 2 の装置との間の経路の信頼性を示すヘッダを前記メッセージに追加し、そのメッセージを第 2 の暗号化通信チャネルを介して第 2 の装置に送信する手段

として機能させるプログラム。

【書類名】 明細書

【発明の名称】 端末間の暗号化通信チャネルを構築するためのセッション管理装置、方法及びプログラム

【技術分野】**【0001】**

本発明は、ネットワーク上の2つの端末間でセキュアなデータチャネルを構築する技術に関するものである。

【背景技術】**【0002】**

従来技術において、IPネットワーク上の2つの端末間でデータチャネルを構築しいわゆるピア・ツー・ピアの通信を行うためには、DNSへの名前登録から、セキュリティを確保するためのFW等の設定・管理、証明書取得等の作業が必要である。また、多数の端末同士の間で相互認証および暗号化されたピア・ツー・ピアの通信を行うためにはそれら全端末の証明書を取得するか、あるいは全端末のID、パスワードを管理することが必要である。

【0003】

また、従来技術として、SIPに基づくシグナリングを行って、2端末間でデータチャネルを確立する技術があるが、このような従来技術において両端末が互いを信頼しながらシグナリングできるようにするためには、例えば両端末間で予め証明書と鍵情報を交換しておくという煩雑な手続きが必要である。

【0004】

上記の通り、従来技術ではセキュアなデータチャネルを容易に構築することはできなかった。

【特許文献1】 特開2002-208921号公報

【発明の開示】**【発明が解決しようとする課題】****【0005】**

本発明は、上記の点に鑑みてなされたものであり、安全にシグナリングを行って端末間でセキュアなデータチャネルを容易に構築するための技術を提供することを目的とする。

【課題を解決するための手段】**【0006】**

上記の課題は、第1の装置及び第2の装置とネットワークを介して接続する手段を備えたセッション管理装置であって、第1の装置との間で相互認証を行い、セッション管理装置と第1の装置との間で第1の暗号化通信チャネルを確立し、第1の装置の名前と第1の暗号化通信チャネルの識別情報とを対応付けて保持する手段と、セッション管理装置と第2の装置との間で相互認証に基づく第2の暗号化通信チャネルを確立する手段と、第1の装置から、第1の装置の名前を含むメッセージを、第1の暗号化通信チャネルを介して受信し、当該メッセージに含まれる第1の装置の名前と、第1の暗号化通信チャネルの識別情報と対応付けて保持されている第1の装置の名前とを比較することにより、メッセージに含まれる第1の装置の名前が正しいか否かを判定する手段と、そのメッセージを第2の暗号化通信チャネルを介して第2の装置に送信する手段とを有することを特徴とするセッション管理装置によって解決できる。

【0007】

本発明によれば、端末が名前を詐称することを防止することができ、安全にメッセージを転送できる。これにより、シグナリングメッセージを安全に転送でき、また、シグナリングメッセージに端末間通信のための鍵情報を含めることにより、端末間でセキュアなデータチャネルを容易に構築することができる。

【0008】

前記メッセージに含まれる第1の装置の名前が正しくないと判定した場合に、エラーメッセージを第1の端末に送信するようにしてもよい。

【0009】

また、上記の課題は、第1の装置及び第2の装置とネットワークを介して接続する手段を備えたセッション管理装置であって、第1の装置との間で相互認証を行い、セッション管理装置と第1の装置との間で第1の暗号化通信チャネルを確立する手段と、セッション管理装置と第2の装置との間で相互認証に基づく第2の暗号化通信チャネルを確立する手段と、第1の装置から、第1の装置とセッション管理装置間の経路の信頼性を示すヘッダを含むメッセージを、第1の暗号化通信チャネルを介して受信する手段と、セッション管理装置と第2の装置との間の経路の信頼性を示すヘッダを前記メッセージに追加し、そのメッセージを第2の暗号化通信チャネルを介して第2の装置に送信する手段とを有することを特徴とするセッション管理装置によっても解決できる。

【0010】

本発明によれば、経路の信頼性を示すヘッダをメッセージに含めるので、メッセージを受信した第2の装置では、ヘッダを確認することにより、経路の信頼性を確認でき、結果としてメッセージの信頼性を確認できる。従って、安全にシグナリングメッセージを転送できる。

【0011】

前記メッセージに含まれる前記経路の信頼性を示すヘッダは、当該ヘッダを付した装置のアドレスを含み、当該メッセージを受信すると、そのヘッダに含まれるアドレスと、当該メッセージを送信した装置のアドレスとを比較することにより、当該ヘッダの正当性を判定するようにしてもよい。

【発明の効果】

【0012】

本発明によれば、名前の詐称を防止し、経路の信頼性を確保ながら安全にシグナリングを行って端末間でセキュアなデータチャネルを容易に構築することができる。

【発明を実施するための最良の形態】

【0013】

以下、本発明の実施の形態を図を参照して説明する。

【0014】

まず、図1を用いて本発明の実施の形態の概要について説明する。

【0015】

図1に示すように、端末1と端末2との間にセッション管理サーバ3を設置し、端末1－セッション管理サーバ3－端末2間で、端末1－端末2間のデータチャネル構築のためのシグナリング（信号手順）を実行し、データチャネル構築後はセッション管理サーバ3を介さずに端末間のみでデータ通信を行うというものである。

【0016】

シグナリングにおいては、まず、端末1－セッション管理サーバ3間、セッション管理サーバ3－端末2間の各々で、IPsec等の暗号化通信を行うためのセキュアシグナリングチャネル確立のために、暗号鍵情報の交換、相互認証が行われる。そして、端末1－セッション管理サーバ3間、セッション管理サーバ3－端末2間の各々で確立されたセキュアシグナリングチャネルを介してセッション管理サーバへの名前登録、端末1－端末2間のセキュアデータチャネル確立のためのシグナリングが実行される。

【0017】

端末1－セッション管理サーバ3間、セッション管理サーバ3－端末2間でのセキュアシグナリングチャネル確立におけるシグナリングにより、セッション管理サーバ3と端末1との間、セッション管理サーバ3と端末2との間において相互認証に基づく信頼関係が確立されているため、端末1と端末2の間でも信頼関係が確立されている。すなわち、上記の相互認証により、セッション管理サーバ3を介した信頼のチェーンモデルが構築される。従って、端末1－端末2間のセキュアデータチャネル確立のためのシグナリングでは、簡易な鍵情報の交換手順を用いることができる。

【0018】

次に、端末1-セッション管理サーバ3-端末2間の通信のシーケンスを図2を参照して説明する。

【0019】

図2に示すシーケンスは、端末1、セッション管理サーバ3、端末2がインターネット等のIPネットワークに接続されたシステム構成を前提とするものである。

【0020】

各端末は、セッション管理サーバ3との間でシグナリングを実行するシグナリング機能、セキュアデータチャネルを介してデータ通信を行うための機能、及びデータ通信を利用して所望のサービスを提供するアプリケーションを備えている。

【0021】

また、セッション管理サーバは、シグナリングを各端末との間で実行するシグナリング機能、端末間の接続許可等を制御する接続ポリシー制御機能、各端末を認証するための認証機能、端末の名前からIPアドレスを取得する名前解決機能、及び、認証のために用いるID、パスワードを格納するデータベースや、名前とIPアドレスを対応付けて格納するデータベース等を備えている。また、名前解決機能として一般のDNSと同等の機能を持たせることもできる。

【0022】

図2に示すように、端末1-端末2間でのセキュアデータチャネル構築にあたり、まず、端末1-セッション管理サーバ3間、端末2-セッション管理サーバ3間の各々でセキュアシグナリングチャネルを構築して、名前の登録を行う。

【0023】

すなわち、端末1-セッション管理サーバ3間でIPsec等の暗号通信で用いる鍵情報（暗号鍵生成用の情報）の交換を行う（ステップ1）。その後、自分のID、パスワードを含む情報を暗号化して相手側に送信することにより、相互に認証を行う（ステップ2）。認証後は、セキュアシグナリングチャネルが確立された状態となり、そのチャネルを用いて、端末1は名前とIPアドレスの登録をセッション管理サーバ3に対して行う（ステップ3）。端末1の通信相手となる端末2とセッション管理サーバ3間でも同様のシーケンスが実行され、端末2の名前とIPアドレスがセッション管理サーバ3に登録される（ステップ4、5、6）。

【0024】

その後、端末1から端末2への接続要求が、セキュアシグナリングチャネルを介して送信される（ステップ7）。接続要求には、端末2の名前と暗号通信用の鍵情報（暗号鍵生成用の情報）が含まれる。接続要求を受信したセッション管理サーバ3は、端末1からの接続要求に関して、端末1が嘘をついていないことをチェックし（発信者詐称チェック）、更に、接続ポリシー制御機能を用いて端末1と端末2の接続が許可されているかをチェックし（ステップ8）、許可されていれば、名前解決機能を用いてデータベースを参照することにより端末2の名前から端末2のIPアドレスを取得し（ステップ9）、セキュアシグナリングチャネルを介して端末2へ接続要求を転送する（ステップ10）。このとき、端末1のIPアドレスも端末2に送信される。端末1と端末2の接続が許可されていなければ、端末1の接続要求は拒否される。このとき、端末2に関する情報は端末1には全く送信されない。発信者詐称チェックについては後により詳細に説明する。

【0025】

接続要求を受信した端末2は、接続要求に対する応答として、暗号通信用の鍵情報を含む応答メッセージをセキュアシグナリングチャネルを介してセッション管理サーバ3に送信し（ステップ11）、セッション管理サーバ3がその応答メッセージを端末1に送る（ステップ12）。このとき、端末2のIPアドレスも端末1に送信される。

【0026】

この手順により、端末1と端末2との間での暗号化通信が可能となる。すなわち、セキュアデータチャネルが確立され、所望のデータ通信が行われる。

【0027】

ステップ1、2及び4、5を経てセキュアシグナリングチャネルが確立されているということは、端末-セッション管理サーバ間で相互に認証が成功しており、信頼関係が成立しているということである。端末1-セッション管理サーバ3間、及び端末2-セッション管理サーバ3間の各々でこのような関係が成立しているので、端末1と端末2との間も相互に信頼できる関係となることから、ステップ7以降は、一般の暗号化通信で用いられる鍵交換手順より簡略化した手順を用いることが可能となっている。

【0028】

上記のシーケンスを実現する手段として、SIP (session initiation protocol) を拡張したプロトコルを用いることが可能である。すなわち、セッション管理サーバ3をSIPプロキシサーバとして機能させ、SIPのメッセージに上記の手順でやり取りされる情報を含ませる。

【0029】

この場合、セキュアシグナリングチャネルの確立及び名前登録のためにREGISTERメッセージを用い、端末1-端末2間のセキュアデータチャネル確立のためにINVITEメッセージを用いることができる。

【0030】

SIPを用いる場合のシーケンス例を図3に示す。

【0031】

図3に示す例は、セキュアなチャネルで接続された複数のセッション管理サーバを経由してシグナリングを行う場合の例である。なお、セキュアなチャネルで接続された複数のセッション管理サーバをセッション管理装置と称する場合がある。図3に示すシーケンスの構成において、端末1のIPアドレスが2001:1234::10、セッション管理サーバAのIPアドレスが2001:6789::5060、セッション管理サーバBのIPアドレスが2001:abcd::5060、端末2のIPアドレスが2001:cd ef::10である。

【0032】

各端末とセッション管理サーバ間では予め互いにID、パスワードを配布しておき、端末とセッション管理サーバの各々は、相手のID、パスワードを自分の記憶装置に格納する。また、セッション管理サーバAとセッション管理サーバBの間は、TLS等のセキュアなチャネルを介して通信を行う。

【0033】

まず、端末1、2は、REGISTERメッセージを用いて、セッション管理サーバとのセキュアチャネルの確立、及び、(SIPに準拠した) 名前の登録をセッション管理サーバA、Bに対して行う(ステップ21)(図2のステップ1~6に相当する)。なお、この部分の手順については後により詳細に説明する。

【0034】

続いて、端末1が、暗号通信用の鍵情報(図の例では秘密共有鍵生成用の情報)をSDPパラメータとして記述したINVITEメッセージを、端末2への接続要求として、端末1とセッション管理サーバA間のセキュアシグナリングチャネルを介して送信する(ステップ22)。セッション管理サーバAは、そのINVITEメッセージをセッション管理サーバA、B間のセキュアなチャネルを介してセッション管理サーバBに転送する(ステップ23)。

【0035】

なお、端末1からのINVITEメッセージにはRoute-Securityヘッダが含まれる。Route-Securityヘッダが付加されている場合、そのINVITEメッセージを受信した装置は、Route-Securityヘッダ:[アドレス]で示されているアドレスから当該装置までの経路がセキュアなものであるかどうか(例えばIPsecによる暗号化がなされているかどうか)をチェックし、セキュアなものであればそのRoute-Securityヘッダをそのまま残してメッセージを転送する。また、転送先で経路がセキュアなものであるかどうかチェックを要する場合には、Route-Securityヘッダ:[自分のアドレス]を付加したメッセージをその

転送先に転送する。応答メッセージには、これまでに付されたRoute-Securityヘッダがそのまま付されており、これにより、メッセージがセキュアな経路を介して転送されたものであることがわかる。すわわち、Route-Securityヘッダにより、経路の安全性を担保する仕組みが提供される。なお、Route-Securityヘッダの種々の形態については後により詳細に説明する。

【0036】

セッション管理サーバBは端末2に、INVITEメッセージを端末2とセッション管理サーバB間のセキュアシグナリングチャネルを介して送信する（ステップ24）。なお、セッション管理サーバA及びセッション管理サーバBにおいて端末2の名前解決がなされている。

【0037】

INVITEメッセージを受信した端末2は、暗号通信用の鍵情報をSDPパラメータとして含む応答メッセージを端末1に向けて送信する（ステップ25）。そして、その応答メッセージは、INVITEメッセージと同じルート上を逆の方向に運ばれ、端末1に送信される（ステップ26、27）。

【0038】

その後、受信確認（ACK）メッセージが端末1から端末2に送信され（ステップ28～30）、端末1と端末2との間の暗号化通信（例えばIPsecによる通信）が可能となる。

【0039】

図3のステップ21におけるREGISTERメッセージのシーケンスは、例えば図4に示す通りである。

【0040】

この場合、まず、暗号通信用（IPsec等）の鍵情報を含むREGISTERメッセージを端末からセッション管理サーバに送信する（ステップ211）。セッション管理サーバはその応答として暗号通信用の鍵情報を含む応答メッセージを端末に返す（ステップ212）。続いて、端末は、セッション管理サーバが端末を認証するための認証用情報を含むREGISTERメッセージをセッション管理サーバに送信する（ステップ213）。セッション管理サーバはその応答として、端末がセッション管理サーバを認証するために必要な認証用情報を含む応答メッセージを端末に送信する（ステップ214）。互いの認証が取れた後、セキュアシグナリングチャネルによる暗号化通信が可能となる。

【0041】

その後は、パケットがセキュアシグナリングチャネルを介して暗号化して送受信されるため、通常のREGISTERメッセージシーケンスにより名前の登録が行われる（ステップ215、216）。

【0042】

なお、上記のシーケンスにおいて、IPsec等の暗号化通信に必要なその他の情報は適宜送受信されているものとする。なお、認証用情報は、ID、パスワード等を含む情報でもよいし、証明書（X.509証明書等）でもよい。また、暗号通信用の鍵情報の交換のために用いるメッセージに認証用情報（証明書）を含めてもよい。

【0043】

（身元詐称監視、ルートの信頼性確認）

さて、これまでに説明したように、端末とセッション管理サーバ間で相互認証を行うことにより、各端末とセッション管理サーバとの間で相互信頼の関係が築け、これにより、セッション管理サーバを介した簡易なシグナリング手順を用いて端末間でセキュアデータチャネルを容易に確立できるようになる。更に本実施の形態では、図3に示したシーケンスにおいて、セキュアデータチャネル構築におけるINVITEメッセージによるシグナリングをよりセキュアに行うために、セッション管理サーバによる身元詐称監視（発信者詐称チェック）、及び、ルートが安全であることを通知するためのRoute-Securityヘッダの付加を行っている。

【0044】

ここで、Route-Securityヘッダについて説明する。前述したように、Route-Securityヘッダは、INVITEメッセージ等のリクエストメッセージの送信の際に、端末(SIP UA)、及び各セッション管理サーバ(SIPプロキシ)にて付加されるヘッダであり、少なくとも自身のIPアドレスを含む。Route-Securityヘッダは、リクエストメッセージの送信に用いる経路(リンクともいう)がセキュアなものであることを送信先に通知する場合に付加する。また、リクエストメッセージを送信しようとするリンクのセキュリティが予め定めたレベル以上である場合に付加するようにしてもよい。

【0045】

Route-Securityヘッダには、リクエストメッセージを次のノードに送信するために用いるリンクのセキュリティ機能に応じた“セキュリティレベル”のパラメータを付加してもよい。例えば、認証(本人性確認)を行わない、認証行う、完全性保証(パケットが改ざんされていないことを保証)、秘密性(パケットの内容を暗号化)、等のレベルに応じて、0~3のパラメータを付加することができる。セキュリティレベル付きのメッセージを受信したノードは、Route-SecurityヘッダのIPアドレスと、前段ノードのIPアドレスとを比較することにより、Route-Securityヘッダが正しく付加されているか否かを判定できるとともに、Route-Securityヘッダに示されたセキュリティレベルが、メッセージを受信したリンクのセキュリティレベルと一致するか否かにより、パラメータが正当なものか否かを判定できる。なお、Route-SecurityヘッダのIPアドレスと、前段のIPアドレスとが一致していない場合に、前段でRoute-Securityヘッダが付加されていなかったものと判定し、前段のIPアドレスを使用して“セキュリティレベル”無しのRoute-Securityヘッダを追加するようにしてもよい。これにより、受信端末で、Route-Securityヘッダが付加されなかったリンクがあることを知ることができる。

【0046】

1つ又は複数のセッション管理サーバを経由してリクエストメッセージを受信した端末(SIP UA)は、メッセージに付加されているRoute-Securityヘッダを参照することにより、例えば、経路中にRoute-Securityヘッダが付加されていないリンクが存在する場合に、安全性の十分でない経路を経由した可能性があることを判断できる。また、セキュリティレベルの低いパラメータを有するRoute-Securityヘッダが含まれている場合、セキュリティレベルが低いリンクを経由したことを判定できる。信頼性が十分でないと判定した場合、例えばエラー応答を返すことができる。

【0047】

また、一連の相互認証に基づくセキュアシグナリングチャネルを介してリクエストメッセージが端末に転送される場合には、各ノードは、前段のノードが正しくRoute-Securityヘッダを付加したか否かをチェックする(例えば、IPアドレスをチェックする)だけでもよい。すなわち、一連のRoute-Securityヘッダが付加されたリクエストメッセージを受信した端末は、その前段のノードが付加したRoute-Securityヘッダをチェックするのみで経路の安全性を信頼する。この場合、例えば、各ノードでは、前段で正しいRoute-Securityヘッダが付加されていないことを検出した場合には、送信元にエラーを返すなどの処理を行う。後に説明する図5、6、7に示す例は、この場合を示している。

【0048】

さて、リクエストメッセージを受信した端末は、受信したリクエストメッセージに含まれるRoute-Securityヘッダを、順序を維持した上でそのまま応答メッセージに含める。応答メッセージは、リクエストメッセージと同じ経路で送信元の端末に転送されるが、経由する各セッション管理サーバでは、例えば、自身が付与したRoute-Securityヘッダに含まれるIPアドレスを、自身のIPアドレスと比較することにより、メッセージをチェックできる。

【0049】

Route-Securityヘッダがそのまま付加された応答メッセージを受信したリクエストメッセージ送信元の端末は、リクエストメッセージを受信した端末と同様にして一連のRoute-

Securityヘッダをチェックすることによりメッセージの信頼性を判定でき、例えば、信頼性が低いと判定した場合にセッションを取りやめることができる。

【0050】

なお、一連の相互認証に基づくセキュアシグナリングチャネルを介してリクエストメッセージが端末に転送される場合には、自身のアドレスが含まれるRoute-Securityヘッダをチェックするのみでもよい。

【0051】

次に、セッション管理サーバによる身元詐称監視、及び、Route-Securityヘッダの使用例について説明するために、図3に示したシーケンスにおけるステップ22～ステップ27の部分の処理をより詳細に説明する。

【0052】

図5にそのシーケンスを示す。図6、7は、図5に示すシーケンスを説明するための図である。以下の説明では、端末1とセッション管理サーバA間、及び端末2とセッション管理サーバB間でのセキュアシグナリングチャネル確立、及び名前とアドレスのセッション管理サーバへの登録は済んでいるものとする（図5のステップ51～54）。

【0053】

まず、図6(a)に示すように、INVITEメッセージがセッション管理サーバAに対して送信される（ステップ55）。INVITEメッセージには、端末1のIPアドレスを含むRoute-Securityヘッダと、接続先（端末2）の名前（To行、user-b@xyz.com）と、送信元（端末1）の名前（From行、user-a@abc.com）を含む。

【0054】

図6(b)に示すように、INVITEメッセージを受信したセッション管理サーバAは、From行にある端末1の名前が正しいか否か（詐称されていないか否か）をチェックする。ここで、セッション管理サーバAは、端末1の名前、IPアドレス、ポート番号、端末1とセッション管理サーバA間のセキュアシグナリングチャネルのコネクションを識別する情報（例えばIPsec SA）を対応付けて保持している。従って、セッション管理サーバAは、INVITEメッセージを受信したコネクション、送信元のIPアドレス等から、INVITEメッセージの送信元の名前を把握でき、その名前と、受信したINVITEメッセージのFrom行にある名前とを比較して、これらが一致した場合に詐称はないものと判断できる。また、同様に、Route-Securityヘッダに含まれるIPアドレスと、上記のコネクションに対応するIPアドレスとを比較して、Route-Securityヘッダが正しく付加されているか否かを判断できる。ここでFrom行もしくはRoute-Securityヘッダが正しくないものである場合には、例えばINVITEメッセージの転送を止め、エラーメッセージを送信元に返すこと等が可能である。

【0055】

なお、端末1とセッション管理サーバA間では相互認証がなされた上でセキュアシグナリングチャネルが設けられているので、セッション管理サーバAは、端末1から受信するINVITEメッセージを端末1から送信されたものであると信頼できる。従って、From行にある名前をチェックすることにより、端末1が詐称を行っていないかどうかをチェックできる。

【0056】

次に、セッション管理サーバAは、自身のIPアドレスを含むRoute-Securityヘッダを追加したINVITEメッセージをセッション管理サーバBに転送する（ステップ56）。セッション管理サーバAとセッション管理サーバB間も端末1とセッション管理サーバA間と同様にセキュアなチャネルで接続されており、セッション管理サーバBは、セッション管理サーバAからそのチャネルを介して送られてきたINVITEメッセージは確かにセッション管理サーバAから送られてきたものであると判断する。そして、セッション管理サーバBは、セッション管理サーバAにおいて追加されたRoute-SecurityヘッダのIPアドレス等をチェックすることにより、Route-Securityヘッダが正しく付加されているか否かをチェックする。

【0057】

続いて、図7(a)に示すように、セッション管理サーバBは、自身のIPアドレスを含むRoute-Securityヘッダを追加したINVITEメッセージを端末2に転送する(ステップ57)。端末2は、Route-Securityヘッダをチェックすることにより、INVITEメッセージが転送されてきた経路の信頼性を確認できる。

【0058】

INVITEメッセージを受信した端末2は、Route-Securityヘッダと、To行、From行をそのまま含む応答メッセージを、INVITEメッセージが転送されてきた経路と逆の経路を辿って送信元に送信する。従って、まず、応答メッセージはセッション管理サーバBに送信される(ステップ58)。

【0059】

端末2から応答メッセージを受信したセッション管理サーバBは、例えば、先頭のRoute-SecurityヘッダのIPアドレスが自身のIPアドレスと一致するか否かを判断することによってメッセージの詐称チェックを行う。そして、応答メッセージはセッション管理サーバBからセッション管理サーバAに転送される(ステップ59)。

【0060】

セッション管理サーバAでは、2番目のRoute-SecurityヘッダのIPアドレスが自身のIPアドレスと一致するか否かを判断することによってチェックを行う。そして、応答メッセージは、INVITEメッセージの送信元である端末1に転送され(ステップ60)、端末1では、3番目のRoute-SecurityヘッダのIPアドレスが自身のIPアドレスと一致するか否かを判断することによってメッセージの正当性をチェックする。また、端末1は、一連のRoute-Securityヘッダを確認することにより経路の信頼性を確認することもできる。ここで、例えば、信頼性の低い経路を経由したと判定した場合には、以降のセッションを中止するといった処理を行うことが可能である。

【0061】

次に、シグナリングプロトコルとしてSIPを用いる場合の各装置の機能ブロックを図8を参照して説明する。

【0062】

セッション管理サーバは、呼(メッセージ)の転送のための処理を行うSIPプロキシ、SIPの名前登録を行うSIPレジストラ、ID、パスワード、もしくは証明書等を用いて各端末の認証を行う認証モジュール、IPsec等の暗号化通信を行うための暗号化モジュールを有している。

【0063】

また、各端末は、セキュアデータチャネル上での通信を行う機能部、INVITEメッセージの送受信やREGISTERメッセージの発行等を含むSIPに基づくメッセージ通信を行うSIP機能部、ID、パスワード、もしくは証明書等を用いてセッション管理サーバの認証を行う認証モジュール、IPsec等の暗号化通信を行うための暗号化モジュールを有している。

【0064】

上記のセッション管理サーバ、各端末の機能は、プログラムにより実現されるものであり、本発明におけるセッション管理装置、端末の各手段は、プログラムと、セッション管理装置、端末のハードウェアとで実現されているものである。また、端末は、CPU、メモリ、ハードディスク等を含む一般的なPC等のコンピュータ、モバイル機器等であり、当該コンピュータ等に上記プログラムをインストールすることにより本実施の形態の端末の機能を実現できる。なお、端末はデジタル家電等でもよい。また、セッション管理サーバは、サーバ等のコンピュータであり、CPU、メモリ、ハードディスク等を含む。当該サーバに上記プログラムをインストールすることにより本実施の形態のセッション管理サーバの機能を実現できる。

【0065】

上記のように本実施の形態のような構成としたことにより、次のような効果を奏する。

【0066】

まず、端末のアドレスが変更される度にREGISTERメッセージによる名前とIPアドレスの登録を行うので、端末側はいわゆる動的IPアドレス割り当てを用いることができる。また、セッション管理サーバが名前解決を行うことから、従来は必要であったオープンなDNSへの名前登録が不要となる。また、各端末とセッション管理サーバ間でセキュアなチャネルを構築してシグナリングを行うので、端末側でのFW管理が不要となる。また、セッション管理サーバが各端末のID、パスワードを管理するので、端末側で多数のID、パスワードを管理することが不要となる。また、セッション管理サーバ接続ポリシー制御機能により、接続を許可していない相手端末に対しては、名前解決さえ許可していないので、その端末の存在自体を知られることがなく、端末が不正なアクセスを受ける恐れがなくなる。更に、セキュアシグナリングチャネルを介したシグナリングにより、セキュアデータチャネルに必要なポート番号が伝えられるので、シグナリングが正常に完了しない場合には、外部にはポート番号を知られることがない。また、軽いシグナリングだけが中間サーバ（セッション管理サーバ）を経由し、実際のデータ通信は端末間でピア・ツー・ピアで行われるので、中間サーバの負荷が過大となることはない。

【0067】

また、従来技術においては、多数の端末同士の間で相互認証および暗号化されたピア・ツー・ピアの通信を行うためにはそれら全端末の証明書を取得するか、あるいは全端末のID、パスワードを管理することが必要であったが、本発明によれば、メンバー同士であれば何の事前セキュリティ設定が不要となる。

【0068】

また、従来技術において、データチャネルの暗号化が不要だったとしても、発番号の信頼性を確保する手段として、PKIを使う方法等しかなかったが、本発明によれば、サービス設定（SIPのID/パスワード設定）だけで発番号の詐称・改竄を防ぐことができる。

【0069】

更に、INVITEメッセージにおけるFrom行の内容の確認を行うことにより、INVITEメッセージの発信元が名前の詐称をしていないかどうかを確認できるようになり、より信頼性を向上させることが可能となる。更に、Route-Securityヘッダを用いることにより、経路の安全性を確認することができ、更に信頼性を向上させることが可能となる。なお、SIPサーバに接続してくる者が必ずしもセキュアなチャネルを通じてきていない場合があることを前提とした場合、名前の詐称確認及びRoute-Securityヘッダによる経路の安全性確認を行うことにより、セキュリティを確保した通信を実現できる。

【0070】

また、実施の形態で説明した詐称確認、Route-Securityヘッダを用いたしくみを用いることにより、他のネットワークを介した場合でも、端末—端末間のセキュアな通信が可能となる。

【0071】

なお、詐称確認、Route-Securityヘッダを用いたしくみをINVITEメッセージを例にとりて説明したが、INVITEメッセージに限られるものでなく、種々のメッセージ転送に適用できる。

【0072】

本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【図面の簡単な説明】

【0073】

【図1】本発明の実施の形態の概要について説明するための図である。

【図2】端末1—セッション管理サーバ3—端末2間の通信のシーケンス図である。

【図3】シーケンスを詳細に示す図である。

【図4】REGISTERメッセージのシーケンスを示す図である。

【図5】身元詐称監視、及びRoute-Securityヘッダを説明するためのシーケンスチャ

ートである。

【図 6】 図 5 のシーケンスを説明するための図である。

【図 7】 図 5 のシーケンスを説明するための図である。

【図 8】 シグナリングプロトコルとして S I P を用いる場合の各装置の機能ブロック

図である。

【符号の説明】

【 0 0 7 4 】

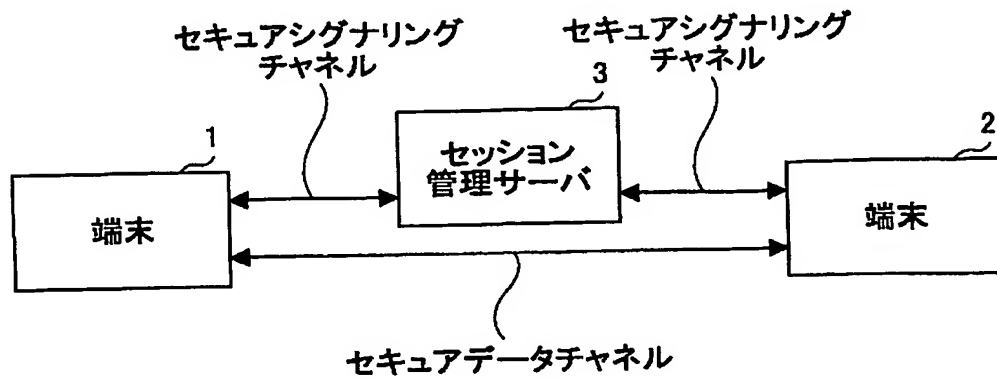
1、 2 端末

3、 A、 B セッション管理サーバ

【書類名】図面

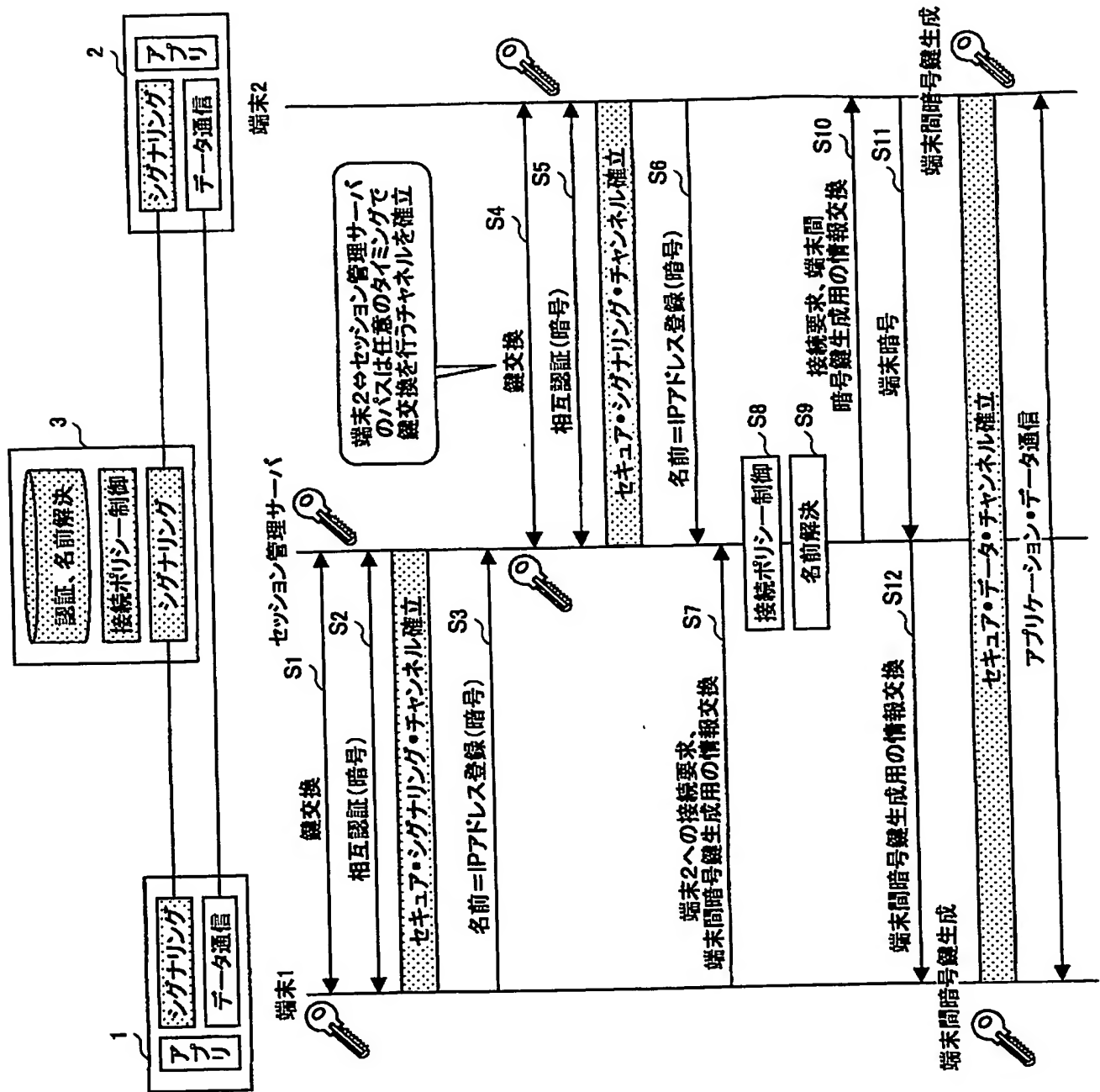
【図 1】

本発明の実施の形態の概要について説明するための図



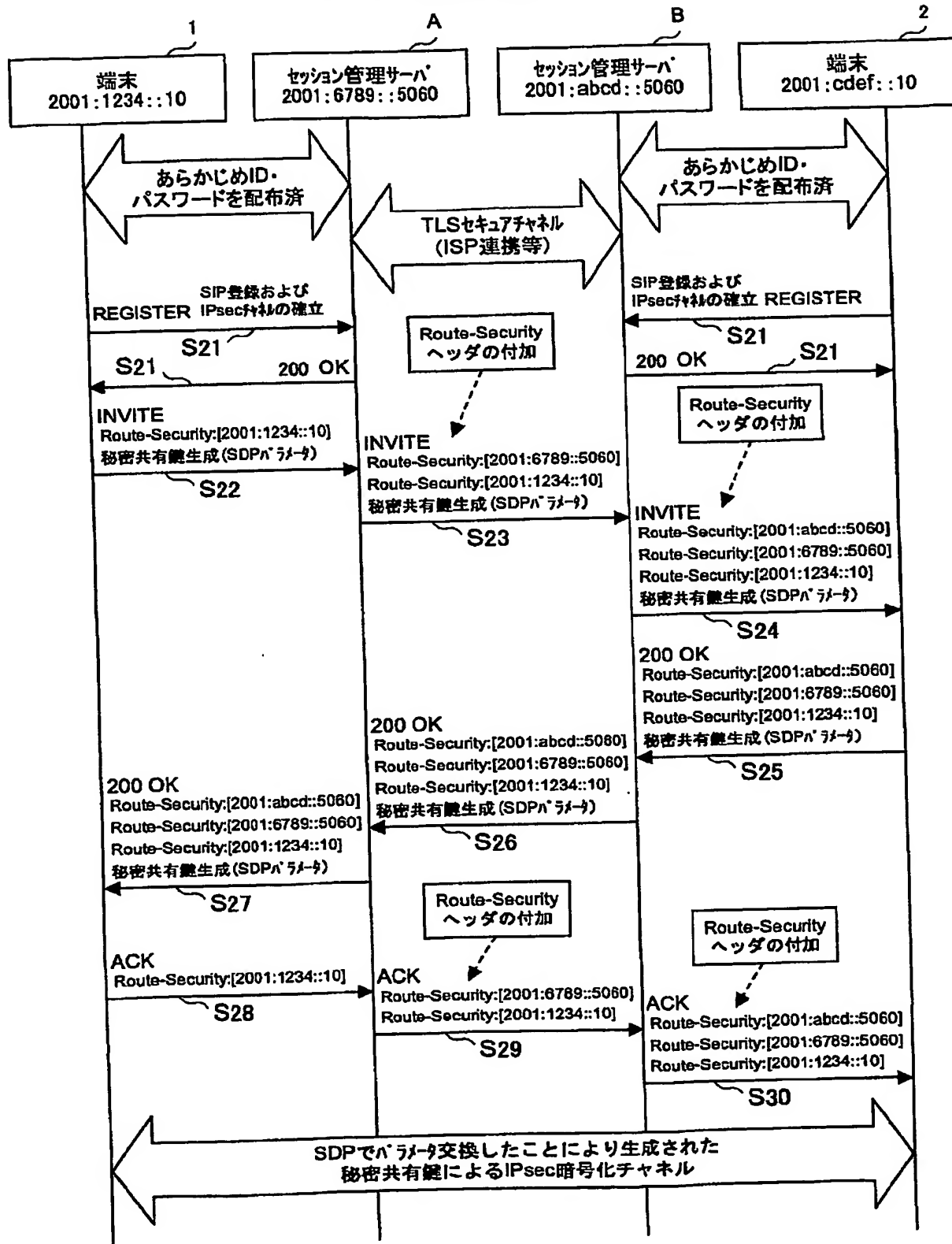
【図2】

端末1-セッション管理サーバ3-端末2間の通信のシーケンス図



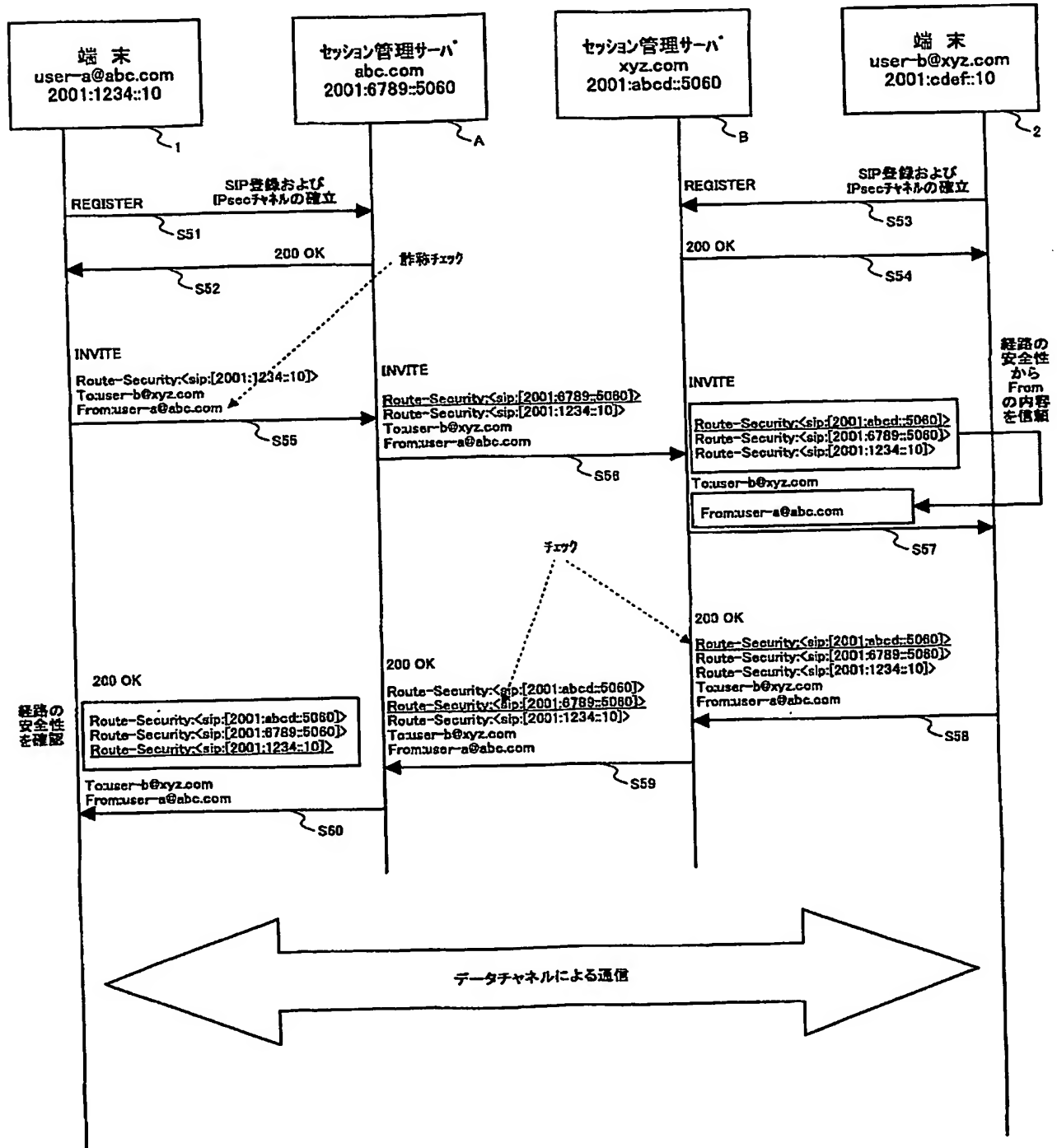
【図 3】

シーケンスを詳細に示す図



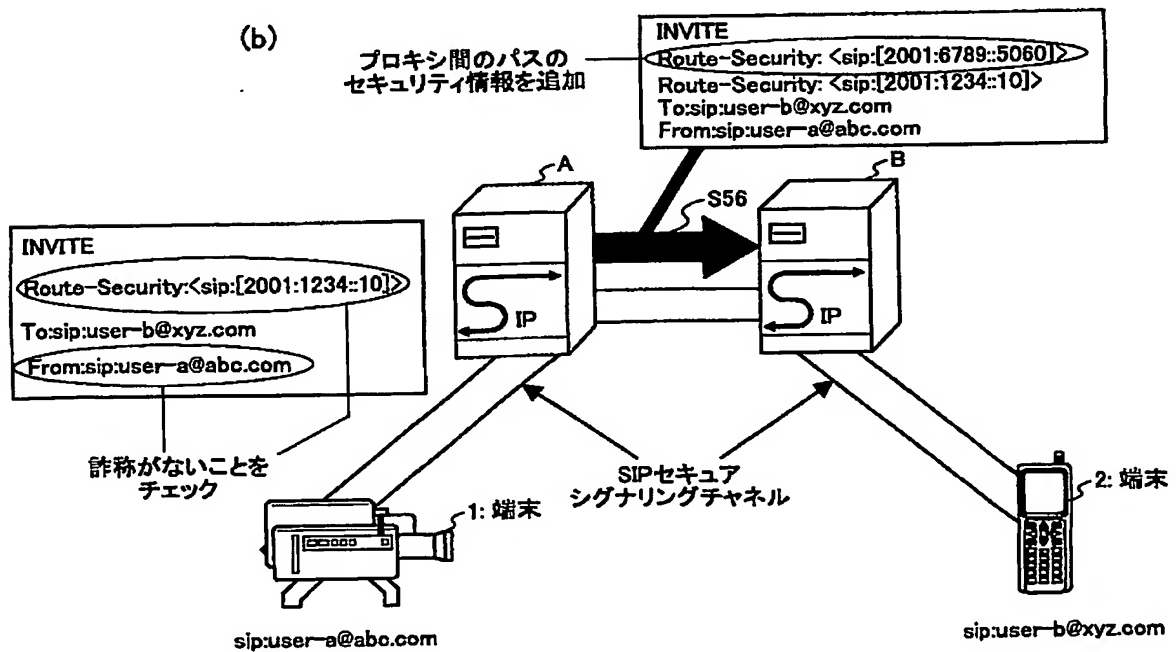
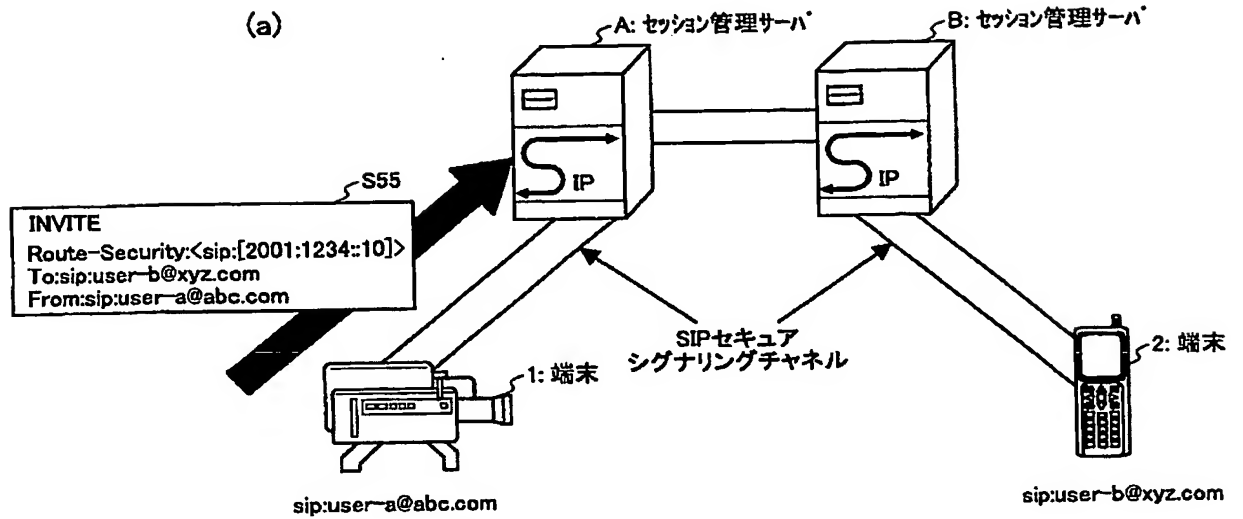
【図 5】

身元詐称監視、及びRoute-Securityヘッダを説明するためのシーケンスチャート



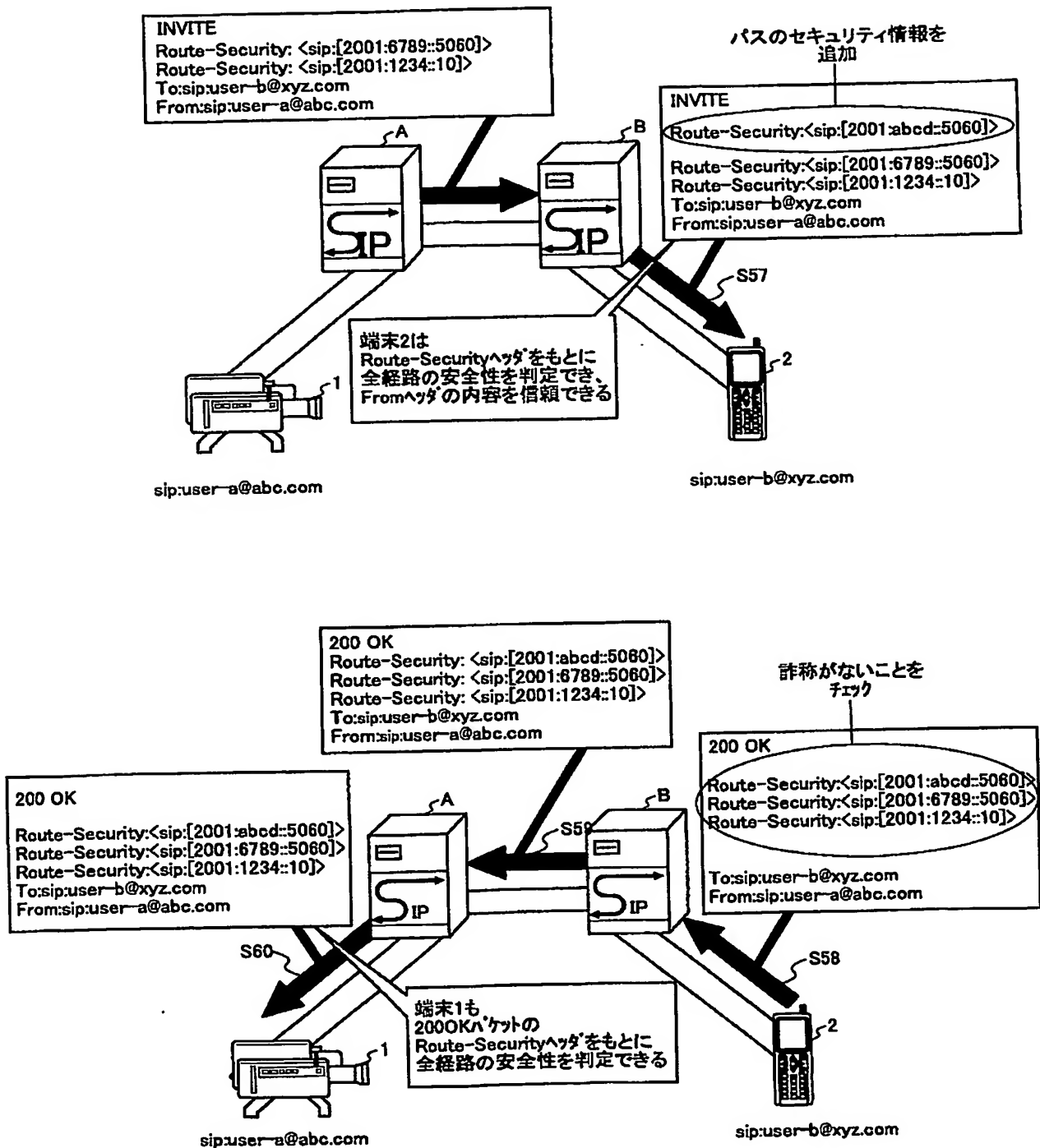
【図 6】

図5のシーケンスを説明するための図



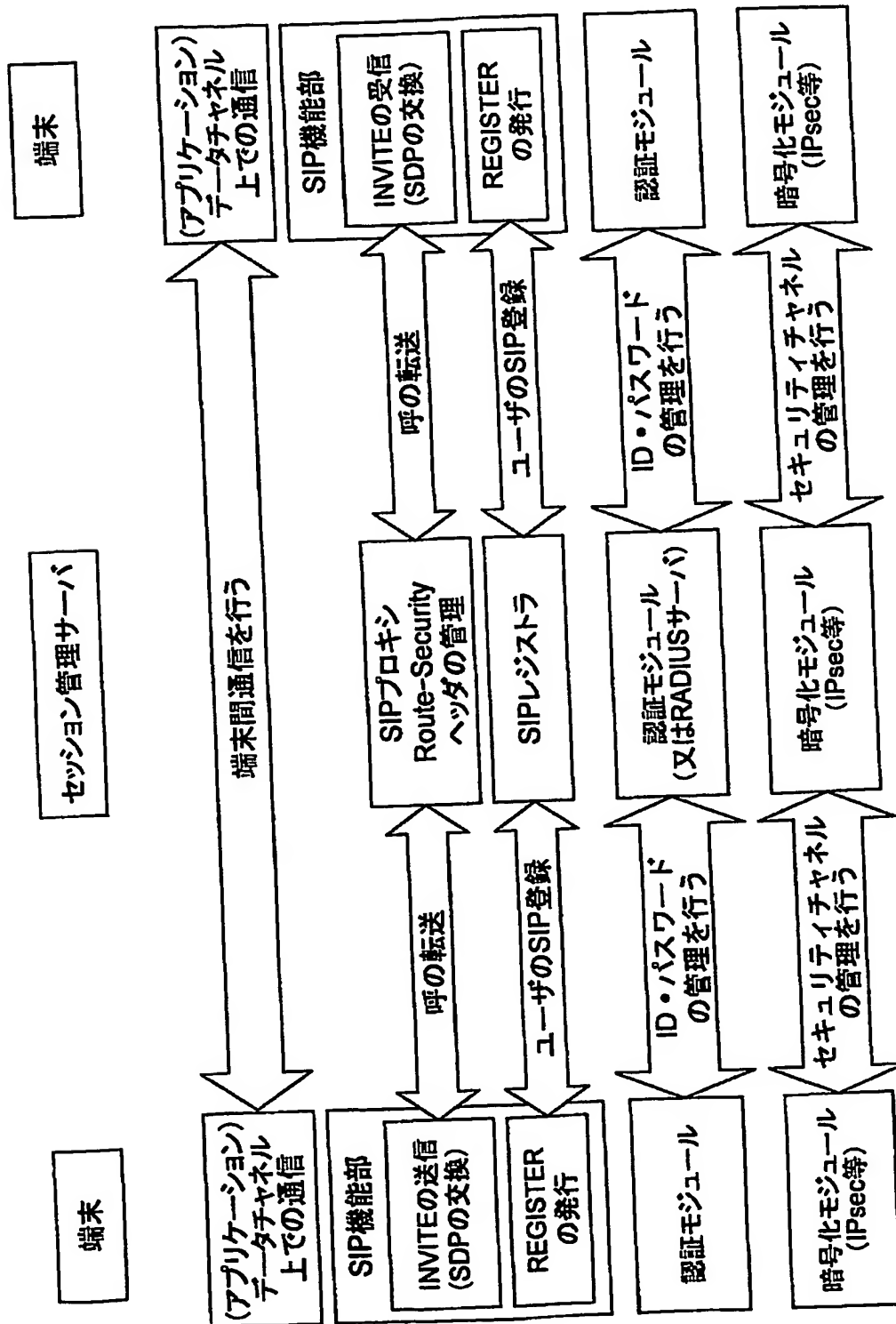
【図 7】

図5のシーケンスを説明するための図



【図 8】

シグナリングプロトコルとしてSIPを用いる場合の各装置の機能ブロック図



【書類名】 要約書

【要約】

【課題】 安全にシグナリングを行って、端末間でセキュアなデータチャネルを容易に構築する。

【解決手段】 第1の装置及び第2の装置とネットワークを介して接続する手段を備えたセッション管理装置において、第1の装置との間で相互認証を行い、セッション管理装置と第1の装置との間で第1の暗号化通信チャネルを確立し、第1の装置の名前と第1の暗号化通信チャネルの識別情報とを対応付けて保持する手段と、セッション管理装置と第2の装置との間で相互認証に基づく第2の暗号化通信チャネルを確立する手段と、第1の装置から、第1の装置の名前を含むメッセージを、第1の暗号化通信チャネルを介して受信し、当該メッセージに含まれる第1の装置の名前と、第1の暗号化通信チャネルの識別情報と対応付けて保持されている第1の装置の名前とを比較することにより、メッセージに含まれる第1の装置の名前が正しいか否かを判定する手段と、そのメッセージを第2の暗号化通信チャネルを介して第2の装置に送信する手段とを備える。

【選択図】 図1

特願 2 0 0 4 - 0 3 7 3 1 4

出 願 人 履 歴 情 報

識別番号

[3 9 9 0 3 5 7 6 6]

1. 変更年月日

1 9 9 9 年 6 月 9 日

[変更理由]

新規登録

住 所

東京都千代田区内幸町一丁目 1 番 6 号

氏 名

エヌ・ティ・ティ・コミュニケーションズ株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record.**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.